ABSTRACT:

In a communication system for a secure transfer of information from a source device to a sink device in a communication session in the form of a plurality of packets from the source device to the sink device, a packet structure is used with a key check block field. During the session, the source device can change the session key used to encrypt data (including the key check block) in the packet. The sink device detects a change of session key by decrypting only the key check block field with a plurality of candidate keys. The key that gave a valid decryption is used for decrypting the remainder of the packet.

Fig. 1